

In The Claims:

1. (Currently Amended) A method of authenticating, using an authentication server, the use of an authentication device by at least a first user over a communication network via an intermediate communication device, comprising:

receiving an interaction request with said intermediate device by said intermediate device from said first user;

responding to said interaction request by said intermediate device, to said first user;

receiving an authentication datagram by said intermediate device, said authentication datagram including data from the first user, in response to said responding;

protecting said datagram by said intermediate device, by at least one of changing, adding to, encrypting and signing of said datagram;

forwarding said protected datagram to said authentication server via the communication network, by said intermediate device, for authentication of the first user; and

continuing interacting with said first user by said intermediate device in response to said authentication;

wherein said intermediate device and said authentication server are separated from one another.

2. (Previously Presented) A method according to claim 1, wherein said intermediate device comprises a vendor World Wide Web site.

3. (Original) A method according to claim 2, wherein protecting comprises adding a signature associated with said vendor to said datagram.

4. (Original) A method according to claim 2, wherein protecting comprises encrypting said datagram.

5. (Previously Presented) A method according to claim 1, wherein said intermediate device comprises a user computing device.
6. (Original) A method according to claim 5, wherein said computing device adds a time stamp to said datagram.
7. (Original) A method according to claim 5, wherein said computing device adds a vendor-associated information item to said datagram.
8. (Original) A method according to claim 5, wherein said computing device encrypts said datagram.
9. (Original) A method according to claim 8, wherein said encryption uses a one time code.
10. (Previously Presented) A method according to claim 8, wherein said one time code is provided by a vendor for a particular session with said user.
11. (Original) A method according to claim 5, wherein said user computing device uses an embedded software component for said protecting.
12. (Original) A method according to claim 11, wherein said embedded software comprises an ActiveX component.
13. (Original) A method according to claim 11, wherein said component is cached on said user device.
14. (Original) A method according to claim 11, wherein said component requires a property value provided by a vendor to operate.

15. (Original) A method according to claim 1, wherein communication between said intermediate device and said server uses a secure connection.

16. (Original) A method according to claim 1, wherein different communication paths are used for said authentication and for transaction details from said user.

17. (Original) A method according to claim 1, wherein different communication paths are used for said authentication and for transaction details from a vendor to said authentication server.

18. (Currently Amended) A method of authentication of an authentication datagram by a remote authentication server, comprising:

sending an encrypted datagram by secure computer communication from a vendor software to said remote authentication server, said encrypted datagram including data from the vendor;

receiving said encrypted datagram by said remote authentication server;

comparing said datagram or a hash thereof to a hash table at said server;

generating a binary validation answer having only a single bit by said server without an associated explanation; and

outputting said binary validation answer for authentication of the vendor;

wherein said vendor software and said remote authentication server are separated from one another.

19. (Previously Presented) A method of authentication of an authentication datagram by a remote authentication server, comprising:

sending an encrypted datagram by computer communication from an authentication device to said remote authentication server, said encrypted datagram including data from at least a first user;

receiving said encrypted datagram by said remote authentication server;

searching, at said server, for a hash value matching said datagram or a hash thereof;

generating a validation answer by said remote authentication server, responsive to said search,

wherein, said datagram includes a secret code and wherein said secret code exists only on said authentication device; and

outputting said validation answer for authentication of the first user;

wherein said authentication device and said remote authentication server are separated from one another.

20. (Original) A method according to claim 19, wherein said authentication device includes a plurality of secret codes that are generated to appear unrelated.

21. (Currently Amended) A method of generating a code set for a remote authentication device, said remote authentication device configured for authentication of at least a first user comprising:

providing a code generating software;

providing at least one seed code for the first user for said software;

generating said code set using said software and said seed;

destroying said seed immediately after generating said code set;

forwarding a first copy said code set to the first user; and

storing a second copy said code set or an indication thereof on said remote authentication device; and

authenticating the first user by matching between said first copy and said second copy or said indication thereof.

22. (Original) A method according to claim 21, comprising generating hash values for said code set.

23. (Original) A method according to claim 22, comprising generating a second set of hash values for said code set, using a different hash function for said second set.

24. (Currently Amended) A method of communication between a vendor and a user using an authentication device, comprising:

generating a one time code for at least the user for a session by a card;

receiving an authentication datagram from at least said user by an intermediate device of a vendor;

forwarding said authentication datagram to a remote authentication server for authentication of the vendor when at least an indication of said one time code that matches the vendor is provided with said datagram; and

forwarding said authentication datagram to said remote authentication server ~~for authentication~~ for authentication of the user when at least an indication of said one time code that matches said user is provided with said authentication datagram;

wherein said intermediate device and said remote authentication server are separated from one another.

25. (Original) A method according to claim 24, comprising signing said datagram using said one time code by said user.

26. (Previously Presented) A method of remote validation of at least a first user, comprising:

from the first user, receiving an authentication datagram by an authentication server from a remote authentication device;

for each datagram received, matching said datagram or a hash of said datagram to a corresponding table;

for each datagram received, calculating a corresponding counter value from a matching position in said corresponding table; and

for each datagram received, if said authentication datagram is valid, increasing said corresponding counter over a previous counter, within a certain limit; and

for each datagram received, outputting a validation signal for the first user, in response to said corresponding counter value.

27. (Original) A method according to claim 26, comprising:

- failing said authentication based on said increase being too large; and
- allowing a subsequent authentication based on a further increase of said subsequent validation being below a second threshold.

28. (Original) A method according to claim 27, wherein said thresholds are the same.

29. (Original) A method according to claim 27, wherein said second threshold is smaller than said certain threshold.

30. (Previously Presented) A method according to claim 26, wherein said counter comprises an ordinal position in said table that is not apparently related to a series of generated random numbers.

31. (Withdrawn) A method of detecting a transmission of an acoustic multitone Frequency Shift Key (FSK) signal from at least a first user comprising:

- receiving an acoustic signal from said at least a first user;
- converting the signal into a Hilbert-transform representation of the signal;
- correlating said converted signal with at least one reference signal representing at least one expected frequency in said FSK signal;
- integrating said correlation over an interval;
- if a signal is present, based on a thresholding of a result of said integrating, generating a validation signal; and
- outputting said validation signal.

32. (Withdrawn) A method according to claim 31, comprising further determining if a detected signal has a frequency within a certain frequency range.

33. (Withdrawn) A method according to claim 31, comprising further determining if a detected signal has a signal to noise ratio within a certain signal to noise ratio range.

34. (Withdrawn) A method according to claim 31, comprising resampling said signal after said determining.

35. (Withdrawn) A method according to claim 31, wherein said threshold is noise dependent of the received signal.

36. (Withdrawn) A method according to claim 31, comprising calculating said interval based on a hardware characteristic of a producer of said acoustic signal.

37. (Previously Presented) A method according to claim 1,
wherein said authentication datagram additionally includes data from a second user; and

wherein said forwarding includes forwarding said datagram to said authentication server for authentication of the second user.

38. (Previously Presented) A method according to claim 18,
wherein said encrypted datagram additionally includes data from a second user; and

wherein said outputting additionally includes outputting said validation answer for authentication of the second user.

39. (Previously Presented) A method according to claim 19,
wherein said encrypted datagram additionally includes data from a second user; and

wherein said outputting additionally includes outputting said validation answer for authentication of the second user.

40. (Previously Presented) A method according to claim 21,
 wherein said remote device is additionally configured for authentication of a second user; and
 wherein said providing at least one seed code additionally includes providing at least one seed code for the second user for said software.
41. (Previously Presented) A method according to claim 26,
 wherein said method is additionally for remote validation of a second user;
 wherein said receiving additionally includes, from the second user, receiving an authentication datagram by an authentication server from a remote authentication device; and
 wherein said outputting additionally includes outputting a validation signal for the second user.
42. (Withdrawn) A method according to claim 31,
 wherein said at least a first user comprises a first user and a second user.
43. (Previously Presented) A method according to claim 2, carried out as part of a commercial interaction between said first user and said vendor, wherein said authentication does not require said first user to interact with a different web server.
44. (Previously Presented) A method according to claim 1, wherein said receiving, protecting and forwarding is secured by a software component which is downloaded to a computing device associated with said first user and used by said user for sending an interaction request.
45. (Previously Presented) A method according to claim 2, wherein said forwarded datagram includes payment instructions to said vendor.

46. (Previously Presented) A method according to claim 44, wherein said forwarding comprises forwarding by said software component.

47. (Previously Presented) A method according to claim 1, wherein said authentication comprises a single bit authentication answer without an associated explanation.

48. (Previously Presented) A method according to claim 21, comprising:

storing said code set or an indication thereof on an authentication server; and
at a later time authenticating said authenticating device by said authentication server by comparing a datagram from said authentication device against said storage at said authentication server.

49. (New) A method according to claim 1, wherein said authentication device comprises a card and wherein said use of an authentication device includes activating the card by pressing a button located on the card.

50. (New) A method according to claim 1, said method further comprising authenticating, using the authentication server, at least the first user by a technique wherein the at least first user is required to input data, the data selected from a PIN, a password, a secret question, voice verification, and a digital signature.